The Language of Engagement and The Influence Objective

By Jesse "Judge" Borque, Lieutenant Colonel, USAF

Editorial Abstract: Lt Col Borque critiques current DOD IO theory, practice and language, and offers an alternative model to current doctrinal conflicts. He proposes a new Strategic Communication construct to simplify both understanding and application of influence operations.

(Opinions expressed in this editorial are those of the author, and do not reflect the official views of the Joint Electronic Warfare Center, JIOWC, or DOD)

Information Operations (IO) isn't irreparably broken. Attempts to employ it within the joint operating environment have simply proven too counterintuitive and contrived to provide a self sustaining —and universally understood—model for effectively conducting the warfare portion of strategic engagement. Much of this stems from its institutionalized misapplication as an organizational model, to the repeated detriment of its apparent design intent as an integrating strategy. From personal experience, when the US Army employs IO they are in fact orchestrating influence operations (or IFO); essentially warfare in cognitive space. The US Air Force speaks of IO largely within the digital sphere, conceiving and testing virtually-derived IO weapons or computer network operations (CNO) tools, versus a broader network-intensive nature or efforts carrying cognitive influence as a first-order effect. This is a fundamentally important distinction between the camps. These cognitive arts (MILDEC, PSYOP, OPSEC) starve when subjected to EW/CNO (or network) organizational subordination, and numerous unfortunate examples describe how the converse is certainly true. Further, we should elevate the broader concept of "network" from that of the strictly computer or cyber, because this essential delineation underscores an institutionally misplaced fact: Electronic Warfare has been conducting true network warfare for its entire existence. Though you must accept that the more permanent uses of "network" were meant to connote command and control (C2) networks, communications networks, integrated air defense system (IADS) networks, supervisory control and data acquisition (SCADA) networks, and a late yet infamous entry: improvised explosive device (IED) networks. Add the new kid "CNO" to the mix and you get the true, full complement of operationalized (USC Title 10) Network Warfare: CNO approaching parity with the mature art of EW to dominate adversary information and control systems.

The current challenge posed by newer "cyber" expressions presents another home-made hurdle for development of convergence language. Find any dictionary or encyclopedia… the prefix "cyber" as an established concept means "of computers." Network in comparison, means "of networks." It's a reasonable bet that the remainder of the English-speaking world (coalition partners, for example) will be reticent to adopt wholesale our politically convenient reinvention of the language. Although the methodology described within the fledgling cyber construct paints a descriptive picture of NW, it effectively requires operators and planners to call yellow "green" from now on, in an arbitrary repackaging of the perfectly adequate, descriptive, and intuitive network concept. In the not-too-distant future, doctrinaires and military philosophers will hopefully realize that not only does "Electromagnetic" Warfare actually encompass "DC to infinity," which by definition also includes the EM energy traveling within a computer network, but that it needn't be constrained by the arcane restriction of free space coupling. CNO would then assume its rightful place as another very powerful subset of EW, just like its grandfather, radar jamming.

The subject of domains of engagement—or simply, "Domains"—constantly provides fodder for doctrinal discussion. A suitable definition of the Domain concept in this context must be useful, objective, and also intuitive to rescue the discussion from a fate of nothing more than a think tank "do" loop. Pragmatically, a Domain must be conceptually or tangibly bounded, complete and continuous within those bounds, with effects delivered within it causally ascertained and reliably, objectively measured. That leaves a bit of real estate in the joint battle space unaccounted for (by these criteria); those ethereal spaces should be secondarily labeled "Environments," as we have commonly seen. So what we have right now for the JFCs' use are the Air, Land, Maritime, and Space Domains, a new "Cyber" Domain bounded by "wired" (non-RF), physically interconnected information processing systems (computers), an Electro-Magnetic Environment (EME) wherein "wireless" EW operations are conducted, and an Information Environment (IE) wherein cognitive operations over any medium are conducted. In this construct, the concept of measurability stands as the delineating characteristic in articulating the two specified environments… that is, until such time that someone can guarantee a reliable stream of "EW BDA" and objectively quantify (not qualify) true changes in foreign or adversary populous' perceptions. Accepting this simple logic, the apparent reason for adopting an over-inclusive Domain (e.g., inclusive of all electrons in transit) may be to assert enhanced ownership within the battle space, not to ensure the delivery of measurable effects for the engaged JFC.

The "wired versus wireless" warfare discussion possesses passionate arguments on both sides, so I'll resort to a simple analogy. Say that dangerous criminals set fire to an occupied building. The building is burning, but only a policeman can get to the fire's location due to the criminal situation. So if a

policeman puts out the fire, is he now a fireman? Of course not… it takes years of seasoning, education, and experience to become an effective policeman, and the firemen (or for that matter, the population) would be much less served were this true. Now, let's say the policeman is the only one who can deny, degrade, deceive, or destroy a WiFi RF link in an adversary computer network… rest assured taxpayers: he's still a policeman.

Shifting briefly to cognitive operations, it's arguably fair to assume agreement on the notion that every observable action yields a cognitive result (or results). For example, one could target (talk to) someone, with predictable cognitive results. Or a force could jam or launch a computer attack against an air defense missile system, with more cognitive results. Or, that force could target (blow up) a power substation with obvious, lasting (and expensive) cognitive results. Although we engage in warfare against adversary cognitive space, information systems, or physical collateral, we may and should employ the latter two mission sets to enable delivery of effects in the cognitive space. However, combining them all using agenda-driven, poorly subordinated architecture in any other way is simple folly, in light of current and projected organizational truths. Unfortunately, this is the current state of IO.

These functionally interrelated but organizationally articulated mission sets are better expressed as Cognitive Warfare (CW), Network Warfare (NW), and Kinetic Warfare (KW), respectively. To continue the theme, one could build a hospital in Country X, serve food to the locals, hand out candy, put on a talent show, or even hold a bake sale there, all with arguably beneficial cognitive results. So why aren't these "missions" core capabilities of IO as well? Although the last snippet was meant in jest, recall that the legitimate battlespace capability of kinetic strike is somehow not a core capability subordinate to IO. This is a conspicuous exclusion for a reason I cannot yet personally fathom, unless the legacy thinking of "kinetic vs other" crept into the creation of a concept that was functionally doomed from the start. In any event, the salient issue here is whether these aforementioned results are intended or not, anticipated or not, and/or catalysts for cascading Nth-order effects, which in turn may be unanticipated, unintended, etc. Further, we must visit whether or not these cognitive results work in concert with standing cognitive enhancement strategies or mitigation strategies, or if we even have such strategies in place to begin with. How many times have I heard from the executive pay grades something along the lines of: "A mosque was just blown up… What kind of IO can we sprinkle on that?"

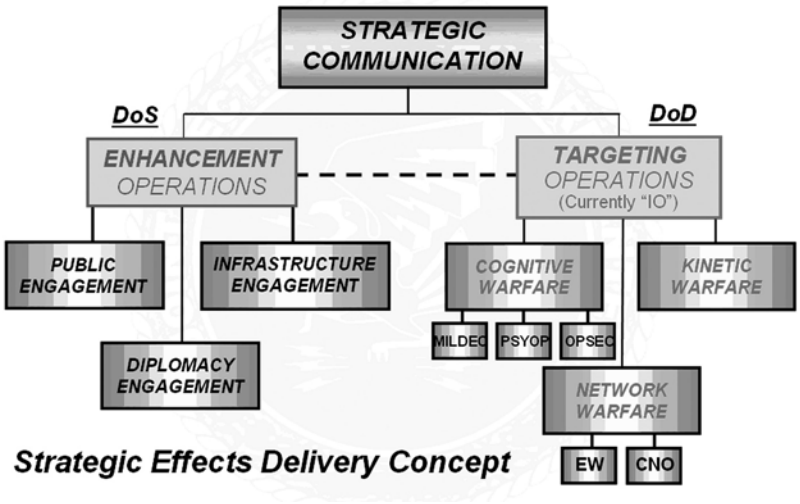

Figure 1. Optimized Strategic Communication model. (Author)

Honestly, the team with the best combined natural IO game (given my experience) are the US Marines. They consider it thoroughly, somehow maintain the requisite finesse during conflict, and arguably demonstrate an uncanny cultural ability to make IO work like a watch. So IO does work? These guys are clearly somehow institutionally and culturally exceptional in this area… I solicit examples to the contrary. In fact, I posit that any of the examples of successful implementation of true, integrated IO in recent operational history serve as exceptions rather than rules. Is it then our aim to promulgate (and expect results from) a doctrine that only those few on the cultural vanguard can implement, or instead to deconstruct the current battlefield truths and reconstruct a simple system that *all* can employ with at least equal effect? Frankly, the Marines will probably still figure out a way to evolve it and overproduce. In short, a military organization shouldn't have to be special just to adhere to the military playbook… that model begs for confusion and inefficiency. I ask those who disagree to closely examine the contributions of IO to the current and lengthy campaign in Iraq, despite the best efforts of otherwise exceptional individuals.

Let me distill a few fundamental notions to make them "operator proof." First, targeting is targeting. It's ultimately no more than an effect to be obtained, delivered by a message, conveyed over a medium. Indeed, it could be as simple as a wish to make an adversary stop advancing toward you (effect), compelling you to send him a 7.62mm round (message) through a barrel (medium). Note the great potential here for cognitive impact. But it needn't be simply kinetic; it should regularly be a bit more complex. For example, you might wish for a certain demographic group to cease building and emplacing IEDs (effect), so you design and execute a persuasive campaign to halt the miscreant activity (message), persistently conveyed via all available print, electronic, or military means (media). This simple language challenges the "targeting is kinetic" paradigm holdouts by describing a universal framework wherein any means

of effects delivery becomes relevant, neither experimental nor intrinsically unsubstantial.

Second, Strategic Communication (SC) should be considered the aggregation of methods the US DOS and DOD use to deliver strategic effects. SC isn't magic, or a mythically holistic game plan, or the sole responsibility of the DOD… State has to begin showing up for the game. Accepting the premise of the previous paragraph is essentially accepting the fact that everything we do constitutes (and hopefully reinforces) Strategic Communication goals by either delivering or enabling delivery of strategic effects. Although some of us work for the DOD and some work for the DOS, we are fundamentally and necessarily united under the auspice of SC… it's not "someone else's job."

Third, within the framework of SC, we then either enhance (or reinforce) positive friendly or adversary behaviors or target (dissuade against or attack) non-compliant adversary behaviors. This framing language is key to simplifying and articulating duties, responsibilities, and missions for the optimized SC model proposed. To capture the full benefit, the designation of some comfortable old standards would change, with the intent of making the model more intuitively available by adequately explaining itself—instead of constantly requiring explanation to facilitate each incidence of employee turnover.

Fourth, and the most fundamental, is to exert engagement pressures, conduct targeting operations, and otherwise emphasize conditions which pull and confine the battlespace into the cognitive domain of engagement at the earliest possible opportunity. That is, reduce engagement to influence as soon as it will probably yield satisfactory anticipated and desired effects. Although I agree that physical engagement of an adversary has an undeniable appeal and will almost certainly remain a viable method of engagement, it is a supporting method of engagement if our ultimate aim is to convince adversaries to comply with our national wishes. This carries an implied task of ensuring freedom of operation within all domains of engagement.

If we accept this simplified view of SC (Figure 1), intuitive parallels naturally emerge. In this model, CW is logically responsible for PSYOP, OPSEC, and MILDEC efforts; NW is responsible for EW and CNO; KW is responsible for conveying physical harm. Where we use "Warfare" to wield the proverbial stick, we may pursue "Engagement" to offer the carrot. CW's complement in the cognitive space is Public Engagement (PE, executed by PA forces), reflecting the statutory prohibitions preventing PSYOP-type operations from being conducted against the American public. Forming a parallel to NW, Diplomacy Engagement (DE) positively engages foreign diplomatic networks to achieve SC objectives. Lastly, Infrastructure Engagement (IE) balances KW, leveraging in-country building and refurbishment efforts to enhance living conditions for the engaged populous, enabling a shift in focus for friendly operations toward the cognitive space. This catalyzes suitable adversary conditions for termination of military operations, and attainment of our desired end state.

To present it all in practical terms, TO effects can only be sanctioned through participation of all three Warfare siblings, and EO effects likewise require participation of all three Engagement siblings to be properly vetted. During several phases of conflict, some siblings from either group will appear underemployed. For example, early in a major combat operation scenario, NW and KW may weigh more heavily than CW operations, ostensibly serving as an "attention step" for adversary decision makers, but primarily to assure required freedom of operation within adversary space. Next, SC will shift focus to CW and IE in order to create favorable conditions, demonstrate goodwill, and serve as a bridging action for transition to end state. As the conflict matures, freedom of operation across the engagement domains is achieved and fundamental conditions previously compelling non-compliant adversary behaviors are addressed and sufficiently neutralized. Further, DE is engaged (or accelerated) to bring closure on favorable terms and foster post-conflict relationships, or possibly even alliances.

In the near term, more practical and meaningful harmonization of engagement concepts and frameworks must occur, both to rightly evolve our fundamental modes of employment and to achieve a more sustainable business model. Simpler, more naturally descriptive models of employment such as the example depicted herein are intrinsically superior, more readily applicable, and more institutionally survivable. After quite some period of challenge and evolution, the wheel remains a good idea.